

# Phase map decompositions for unitaries

Niel de Beaudrap<sup>1</sup>, Vincent Danos<sup>2</sup>, and Elham Kashefi<sup>1</sup>

<sup>1</sup> IQC, University of Waterloo

<sup>2</sup> CNRS, Université Paris 7

**Abstract.** We propose a universal decomposition of unitary maps over a tensorial power of  $\mathbb{C}^2$ , introducing the key concept of *phase maps*, and investigate how this decomposition can be used to implement unitary maps directly in the measurement-based model for quantum computing. Specifically, we show how to extract from such a decomposition a matching entangled graph state (with inputs), and a set of measurements angles, when there is one. Next, we check whether the obtained graph state verifies a *flow* condition, which guarantees an execution order such that the dependent measurements and corrections of the pattern yield deterministic results. Using a graph theoretic characterization of flows, we can determine whether a flow can be constructed for a graph state in polynomial time. This approach yields an algorithmic procedure which, when it succeeds, may produce an efficient pattern for a given unitary.

## 1 Introduction

Measurement-based quantum computing [1,2,3,4] has attracted considerable interest in quantum computing research during the last few years. Different aspects of this model have been investigated, including: characterization of the initial entangled states [5,6,7,8,9,10], description and unification of different models [11,12,13,14,15,16,17,18], investigation of fault tolerant computing within this framework [19,20,21,22,23,24,25], and proposals for implementations [26,27,28,29,30,31,32,33,34,35].

It remains an open question however, whether this model may suggest new techniques for designing quantum algorithms. This is the question we address in the present paper. Specifically, we introduce a methodology for the direct decomposition of a given unitary map into a one-way model pattern.

Previously, one would typically start with an algorithm already implemented in the circuit model, replace each gate by a corresponding pattern. To transform the pattern to a standard form where all entangling operations are performed first, one could then use the by-product method [3] or the more general standardization algorithm [16]. In this paper, we propose a direct method that is free from any reference to the circuit model. We start with the observation that one-way patterns implicitly define a particular decomposition of unitary maps into a preparation map enlarging the input space, a diagonal map with unit coefficients, and a restriction map contracting back the space to the output space, which we call a *phase map decomposition*. (Note that this decomposition does not directly correspond to any physical procedure.)

Since the one-way model is universal, this alternative decomposition is also universal; and there is a straightforward procedure which allows us to determine a phase map

decomposition for a unitary from a pattern implementing the same unitary. Remarkably, one can define a reverse procedure as well, which breaks in two steps. First, given a unitary map, one enumerates such phase map decompositions by constructing the right set of coefficients in the middle diagonal map (Lemma 2 and Algorithm 1). Then for each such decomposition, one verifies whether there exists a matching one-way pattern. This reduces to finding for any phase map decomposition a matching entangled graph state (with inputs) and choice of measurements angles (Algorithm 2). To obtain the execution order of the one-way pattern, we look for a “flow” for the underlying entanglement graph which describes an adequate set of dependent measurements and corrections so that the obtained pattern is deterministic (Theorem 1). Using a graph theoretic characterization of flows, we can determine whether a flow can be constructed for a graph state in polynomial time (Algorithms 3 and 4).

This constitutes a method for the implementation of unitary maps in the one-way model which bypasses completely the circuit picture, and may produce more efficient implementations in particular instances.

## 2 Preliminaries

We first briefly review the one-way model and the various notions relevant to this paper.

### 2.1 One-way Model

Computations involve a combination of one-qubit preparations  $N_i$ , two-qubit entanglement operators  $E_{ij} := \wedge Z_{ij}$ ,<sup>1</sup> one-qubit measurements  $M_i^\alpha$ , and one-qubit Pauli corrections  $X_i, Z_i$  (where  $i, j$  represent the qubits on which each of these operations apply, and  $\alpha$  is a parameter in  $[0, 2\pi]$ ). A preparation  $N_i$  prepares auxiliary qubit  $i$  in state  $|+\rangle_i$ . An entangling operator  $E_{ij}$  entangles qubits  $i$  and  $j$ . A destructive measurement  $M_i^\alpha$  is defined by the pair of orthogonal projections  $\langle \pm_\alpha |_i$  applied at qubit  $i$ , where  $|\pm_\alpha\rangle$  stand for  $\frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\alpha}|1\rangle)$ . We use the convention that  $\langle +_\alpha |_i$  corresponds to the outcome 0, and  $\langle -_\alpha |_i$  corresponds to 1. Since qubits are measured at most once in a pattern, we may unambiguously represent the outcome of the measurement done at qubit  $j$  by  $s_j$ . The dependent corrections used to control non-determinism are then  $X_i^{s_j}$  and  $Z_i^{s_j}$ , with  $s_j \in \{0, 1\}$ .

A *pattern* is defined by the choice of a finite set  $V$  of qubits, two possibly overlapping subsets  $I$  and  $O$  determining the pattern inputs and outputs, and a finite sequence of commands acting on  $V$ . We require that no command depends on an outcome not yet measured; that no command acts on a qubit already measured; and that a qubit is measured (or prepared) if and only if it is not an output (respectively an input).

Let  $\mathcal{H}_I$  ( $\mathcal{H}_O$ ) denote the Hilbert space spanned by the inputs (outputs). The execution of a pattern consists of performing each command in sequence. If  $n$  is the number of measurements (*i.e.* the number of non-output qubits), then this may follow  $2^n$  different computational branches. Each branch is associated with a unique binary string  $s$  of length  $n$ , representing the classical outcomes of the measurements along that branch,

---

<sup>1</sup> The symmetric operator of controlled- $Z$ .

and a unique *branch map*  $A_s$  representing the linear transformation from  $\mathcal{H}_I$  to  $\mathcal{H}_O$  along that branch. (Note that states resulting from a measurement *are not* normalized.) The branch corresponding to the classical outcomes  $s = 0 \cdots 0$ , will be called the *positive branch*.

A pattern is said to be *deterministic* if all of the branch maps are equal: any given unitary can be implemented by a deterministic pattern (in the precise sense of Theorem 1 below). A pattern is said to be in *standard form* if entangling operators  $E_{ij}$  appear first in its command sequence. Any given pattern can be put in such a form, which reveals implicit parallelism in the computation, and suits certain implementations well [16]. One can then define an *entanglement graph* associated to the initial preparation and entanglement step, with vertices  $V$  and edges  $E_{ij}$ . By doing so, the computation of the pattern can be understood as the direct manipulation of such multipartite entangled states (which are called graph states in the case where there are no inputs).

## 2.2 Geometries and Flows

In order to find a pattern for a given phase map decomposition of a unitary operator, we will need to search for a matching entanglement graph and write the pattern directly from the obtained graph. We may do this using *flows* [36], which we review now.

A *geometry*  $(G, I, O)$  consists of an undirected graph  $G$  together with two subsets of nodes  $I$  and  $O$ , called inputs and outputs. We write  $V$  for the set of nodes in  $G$ ,  $I^c$ , and  $O^c$  for the complements of  $I$  and  $O$  in  $V$ . We write  $x \sim y$  and  $xy \in G$  when  $x$  is adjacent to  $y$  in  $G$ , and  $E_G := \prod_{xy \in G} E_{xy}$  for the global entanglement operator associated to  $G$ . (Note that all  $E_{xy}$  commute so the order in this product is irrelevant.) To extend a geometry into a pattern, it remains only to decide the angles which are used in measuring qubits of  $O^c$ , and the dependent corrections to be used; thus every pattern has an underlying geometry which is obtained by forgetting the measurements and corrections.

We give now a condition on geometries under which one can synthesize a set of dependent corrections such that the obtained pattern is deterministic.

**Definition 1** A flow  $(f, \preceq)$  for a geometry  $(G, I, O)$  consists of a map  $f : O^c \rightarrow I^c$  and a partial order  $\preceq$  over  $V$  such that for all  $x \in O^c$ :

- (Fi)  $x \sim f(x)$ ;
- (Fii)  $x \preceq f(x)$ ;
- (Fiii) for all  $y \sim f(x)$ , we have  $x \preceq y$ .

The coarsest order  $\preceq$  for which  $(f, \preceq)$  is a flow will be called the *dependency order* induced by  $f$ .

**Theorem 1 ([36])** Suppose the geometry  $(G, I, O)$  has flow  $f$ , then the pattern:

$$\mathcal{P}_{f,G,\alpha} := \prod_{i \in O^c}^{\preceq} \left( X_{f(i)}^{s_i} \prod_{\substack{k \sim f(i) \\ k \neq i}} Z_k^{s_i} M_i^{\alpha_i} \right) E_G N_{I^c}$$

where the product follows the dependency order  $\preceq$  of  $f$ , is deterministic, and realizes the unitary embedding:

$$U_{G,I,O,\alpha} := 2^{|O^c|/2} \left( \prod_{i \in O^c} \langle +_{\alpha_i} | i \rangle \right) E_G N_{I^c}$$

That is: if a geometry has a flow, we may without loss of generality consider only its positive branch. Then measurement-based computing downs to *projection-based* computing. This will be handy in the formulation of our procedure.

### 3 One-way Patterns as Phase Maps

With our preliminaries in place, we now turn to the formulation of our decomposition. Various operators over  $\mathcal{H}$  preserve the computational basis, up to phase: for example, Pauli maps,  $Z^\alpha$  (defined as  $Z^\alpha|0\rangle = |0\rangle$ , and  $Z^\alpha|1\rangle = e^{i\alpha}|1\rangle$ ), and controlled-Paulis. One-qubit measurements also map the standard basis of one space to those of another, up to a scalar factor. In particular, one has the following simple equations where  $|x\rangle$  is an  $n$ -qubit computational basis state and  $j$  is an index for a qubit in  $|x\rangle$ :

$$\begin{aligned} \langle \pm_\alpha | \otimes I^{\otimes n} (|0\rangle|x\rangle) &= 2^{-1/2} |x\rangle \\ \langle \pm_\alpha | \otimes I^{\otimes n} (|1\rangle|x\rangle) &= \pm 2^{-1/2} e^{-i\alpha} |x\rangle \\ \wedge Z_{1j} |0\rangle|x\rangle &= |0\rangle|x\rangle \\ \wedge Z_{1j} |1\rangle|x\rangle &= Z_j |1\rangle|x\rangle \end{aligned}$$

We will call a map  $\Phi : \mathcal{H}_V \longrightarrow \mathcal{H}_V$  a *phase map* if it is diagonal in the computational basis and has only unit coefficients. The typical example of such a map is  $\wedge Z$ . It is important to note that the above definition depends on the choice of a basis.

Following one-way model terminology we also define a *preparation map*  $P_{I \rightarrow V} : \mathcal{H}_I \rightarrow \mathcal{H}_V$  that expands the input space by tensoring auxiliary qubits,

$$|x\rangle \longmapsto |x\rangle \otimes |+\cdots+\rangle_{I^c} ,$$

and a *restriction map*  $R_{V \rightarrow O} : \mathcal{H}_V \rightarrow \mathcal{H}_O$  that projects the space to the output space:

$$|x\rangle \longmapsto \langle +\cdots+ |_{O^c} |x\rangle .$$

It is easy to see that the restriction map is the adjoint of the preparation map.

As we have seen above, measurement and entangling commands in the one-way model define phase maps, and hence from the universality of the model we obtain the following decomposition:

**Theorem 2** *For all unitary  $U : \mathcal{H}_I \longrightarrow \mathcal{H}_O$ , there exists a phase map  $\Phi : \mathcal{H}_V \longrightarrow \mathcal{H}_V$  such that:*

$$U = R_{V \rightarrow O} \circ \Phi \circ P_{I \rightarrow V}$$

**Proof.** We know that  $\wedge Z$  and  $J_\alpha$  are universal [37], and also that compositions of patterns having flows, themselves have a flow [36]. Hence there is a deterministic pattern  $\mathcal{P}$  implementing  $U$ , and from Theorem 1 we then have:

$$\begin{aligned}
U &= 2^{|O^c|/2} \prod_{i \notin O} \langle +_{\alpha_i} |_i E_G P_{I \rightarrow V} \\
&= 2^{|O^c|/2} \prod_{i \notin O} \langle + |_i Z_i^{-\alpha_i} E_G P_{I \rightarrow V} \\
&= R_{V \rightarrow O} \prod_{i \notin O} Z_i^{-\alpha_i} E_G P_{I \rightarrow V} \\
&= R_{V \rightarrow O} \Phi_{V \rightarrow V} P_{I \rightarrow V}
\end{aligned}$$

where  $\Phi = \prod_{i \notin O} Z_i^{-\alpha_i} \prod_{ij \in E} \wedge Z_{ij}$  is the phase map corresponding to the entanglement operations and measurement angles.  $\square$

One can think of the above theorem as a special kind of diagonalization for unitaries where one is allowed to inflate the dimension of the underlying space. This will prove to be useful for direct programming in the one-way model. We present first a couple of examples, clarifying our first set of definitions and preparing the ground for a direct proof of the above theorem which does not invoke universality of the one-way model. This then leads to an algorithm for pattern design. The examples already hint at the construction behind the direct phase map decomposition algorithm.

### 3.1 Example 1

Consider the unitary map  $J_\alpha : \mathcal{H}_{\{1\}} \longrightarrow \mathcal{H}_{\{1\}}$  which decomposes in the computational basis as:

$$J_\alpha = 2^{-1/2} \begin{pmatrix} 1 & e^{-i\alpha} \\ 1 & -e^{-i\alpha} \end{pmatrix} = \begin{pmatrix} 1 & 0 & e^{-i\alpha} & 0 \\ 0 & 1 & 0 & -e^{-i\alpha} \end{pmatrix} \cdot 2^{-1/2} \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}$$

This decomposition is obtained from the one-way pattern  $X_2^{s_1} M_1^\alpha E_{12}$  which implements  $J_\alpha$ , and has as positive branch the phase map:

$$2^{1/2} \langle +_\alpha |_1 \wedge Z_{12} : \mathcal{H}_{\{1,2\}} \longrightarrow \mathcal{H}_{\{2\}}$$

Factoring out the restriction operator gives the decomposition:

$$J_\alpha = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{-i\alpha} & 0 \\ 0 & 0 & 0 & -e^{-i\alpha} \end{pmatrix} \cdot 2^{-1/2} \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}$$

where the left matrix is the restriction  $R_1 : \mathcal{H}_{\{1,2\}} \longrightarrow \mathcal{H}_{\{2\}}$ .

Note that this decomposition is not physical, since the phase map doesn't directly correspond to any operation. Indeed it is a convention to substitute the physically meaningful equation  $\langle +_\alpha | \otimes I(|1\rangle|1\rangle) = 2^{-1/2} e^{-i\alpha} |1\rangle$  with:

$$R_1(2^{-1/2} e^{-i\alpha} |1\rangle|1\rangle) = 2^{-1/2} e^{-i\alpha} |1\rangle$$

However, the corresponding one-way pattern is a physical procedure that may be understood in terms of the above decomposition.

The phase map here is  $Z_1^{-\alpha} \wedge Z_{12}$ , and the decomposition above can be rewritten:

$$J_\alpha = R_1(Z_1^{-\alpha} \wedge Z_{12})P_2$$

As we have seen in the proof above, this reasoning is perfectly general; indeed for any pattern, one gets the phase map associated to the positive branch:

$$\Phi = \prod_{i \in O^c} Z_i^{-\alpha_i} \prod_{ij \in E} \wedge Z_{ij}$$

and writing  $U$  for the corresponding unitary (assuming the pattern does compute a unitary map):

$$U = R_{O^c} \left( \prod_{i \in O^c} Z_i^{-\alpha_i} \prod_{ij \in E} \wedge Z_{ij} \right) P_{I^c}$$

### 3.2 Example 2

Example 1 uses only one auxiliary qubit, and as such is a special case where the required number of auxiliary qubits is equal to the number of inputs. This is of course not always the case and the general algorithm for phase map decomposition will take care of this. We will present exact bounds on how much one needs to expand the computational space to be able to obtain the decomposition; however to realize a decomposition as a pattern we will need further restrictions. The following example demonstrate this case.

The shortest known pattern for the  $Z^\alpha$ -rotation is  $X_3^{s_2} Z_3^{s_1} M_2^0 M_1^{-\alpha} E_{12} E_{23}$  with positive branch:

$$\langle +|_2 \langle +_{-\alpha}|_1 E_{12} E_{23}$$

which induces the 3-qubit phase map  $\Phi|xyz\rangle = (-1)^{xy+yz} e^{i\alpha y} |xyz\rangle$  (indeed a diagonal of units) and corresponds to the following decomposition of  $Z^\alpha$ :

$$R_{12} D(1, 1, 1, -1, e^{i\alpha}, e^{i\alpha}, -e^{i\alpha}, e^{i\alpha}) P_{23}$$

where  $D(\dots)$  is a diagonal matrix. Note that some permutations of the diagonal lead to other solutions, and most decompositions won't correspond to a pattern. Also if one uses only 1 additional qubit one obtains another decomposition with middle map:

$$D(\sqrt{2}, 0, 0, \sqrt{2}e^{i\alpha})$$

which is not a phase map since coefficients are not units. The natural question is whether it is possible to generate all such decompositions without using a pattern, and next find a pattern matching one of these decompositions.

## 4 Direct Decomposition

There is no *a priori* reason why a phase map decomposition could not be obtained without any reference to the one-way model: indeed, it is possible to give a direct approach. Supposing one adds  $n$  auxiliary qubits to the input space  $I$ , a simple calculation shows that for each coefficient  $u$  in the computational basis matrix representation of  $U$ , there will be  $2^{|V|-|O|}/2^{|I|} = 2^{n-|I|}$  ‘slots’ to spread over the diagonal of the phase map  $\Phi$  (since  $U$  is a unitary  $|I| = |O|$ ). Thus, finding a decomposition amounts in this case to finding complex numbers  $x^{(i)}$  such that the following two conditions hold:

$$u = \sum_{i \leq 2^{n-|I|}} x^{(i)} \quad (1)$$

$$2^{n/2} |x^{(i)}| = 1 \quad (2)$$

The first equation says that the restriction map  $R$  will sum up all the  $x^{(i)}$ s to give  $u$ , while the second one asks for unit diagonal elements (note that the preparation map of  $n$  auxiliary qubits introduces an overall factor of  $2^{-n/2}$ ).

**Lemma 2** *If  $n > |I|$ , Equations 1 and 2 have joint solutions iff  $|u| \leq 2^{n/2-|I|}$ .*

**Proof.** Each complex  $x^{(i)}$  can be seen as a real plane vector of constant length  $2^{-n/2}$ , and all one has to do is to choose their angles in a way that they will globally add up to  $u$ . If one aligns all  $x^{(i)}$ s with  $u$ , the resulting sum is at least as long as  $u$  iff  $|u| \leq 2^{n/2-|I|}$ ; thus this inequality is necessary for Equations 1 and 2 to have joint solutions.

If  $n > |I|$ , then  $2^{n-|I|} \geq 2$ , so there are at least two terms  $x^{(i)}$ . We may pick any two of them and rotate them at opposite angles  $\pm\theta$ . If  $\theta$  reaches  $\frac{\pi}{2}$  before the global sum matches  $u$ , then the corresponding two  $x^{(i)}$ s contribute nothing, and we pick two additional terms to rotate. Clearly, at some stage, for some value of  $\theta$  the sum will coincide with that of  $u$ .  $\square$

Due to the unitarity of  $U$ ,  $|u| \leq 1$ : so a safe choice of  $n$  is one such that  $2^{n/2-|I|} \geq 1$ . Thus,  $n \geq 2|I|$  is always sufficient for a phase map to exist. Another consequence of the above lemma is that for any given unitary map  $U$  on  $|I|$  qubits, unless  $U$  is itself a phase map and also requires no auxiliary qubits, we have  $n > |I|$ : then a lower bound on the number of required qubits to implement it as a one-way pattern is  $2|I|$ , if at least one coefficient of  $U$  is larger than  $\frac{1}{2}$ .

For a unitary  $U$ , once we have fixed  $n$ , an output space  $O$ , and a choice of  $x_{pq}^{(i)}$  satisfying Equations 1 and 2 for the coefficients  $u_{pq} = \langle p|U|q \rangle$ , the following algorithm will enumerate all possible decompositions:

**Algorithm 1** Input: for sets  $V$ ,  $I$ , and  $O$  and  $n = |I^c|$ :

- a unitary  $U$  on  $\mathcal{H}_I$ ;
- complex numbers  $\{x_{pq}^{(i)}\}_{i=1}^{2^{n-|I|}}$  satisfying Equations 1 and 2 for each  $u_{pq}$ ;
- a permutation  $\sigma$  over  $\{1, \dots, 2^{n-|I|}\}$ .

Output: diagonal elements  $\{d_{kk}\}_{k=1}^{2^{|V|}}$ , such that  $d_{kk} = \sqrt{2^n} x_{pq}^{(i)}$ , where:

- the binary representation of  $p$  agrees with that of  $k$  after restriction to  $O$ ;

- $q \equiv k \pmod{2^{|I|}};$
- $i = \sigma(\lfloor k/2^{|I|} \rfloor).$

The elements  $\{d_{kk}\}_{k=1}^{2^n}$  are the solution of  $R\Phi P = U$  where  $\Phi = D(d_{11}, d_{22}, \dots);$  due to the simple structure of matrices  $R$  and  $P$  we derive the above algorithm.

Note that obtaining a decomposition is not sufficient for the existence of a pattern. We now discuss how to extract an entanglement graph and measurement angles from a phase map, if there is one.

## 5 Pattern Design

To determine whether a phase map decomposition  $R\Phi P$  of a unitary  $U$  has a corresponding pattern in the one-way measurement model, one wants a graph  $G_E$  over  $V$ , and angles  $\alpha_j$  for  $j \in O^c$  such that

$$\Phi = \prod_{j \in O^c} Z_j^{-\alpha_j} \prod_{jk \in E} \wedge Z_{jk}$$

That means for all  $x$  in the  $V$ -computational basis:

$$d_{xx} = e^{-i \sum_{O^c} \alpha_j x_j} (-1)^{\sum_{jk \in E} x_j x_k} \quad (3)$$

where  $d_{xx}$  is the diagonal coefficient of the phase map corresponding to  $x$  basis. Based on this observation we propose the following algorithm for the above graph matching problem.

**Algorithm 2** Input: A phase map decomposition for  $U$  — i.e. the diagonal elements  $\{d_{xx}\}_{x=1}^{2^{|V|}}$  from Algorithm 1.

Output: either (i) A graph  $G$  on  $V$  and a set of angles of measurements  $\{\alpha_j\}_{j \in O^c}$ , or (ii) no matching graph exists.

1. For  $j \in \{1, \dots, |O^c|\}$ , consider the  $|V|$ -bit string  $\mathbf{z}_j$  that only has a 1 at position  $j$ , and set  $\alpha$  such that  $e^{-i\alpha_j} = d_{\mathbf{z}_j \mathbf{z}_j}$ .
2. For all  $j, k$ , consider the  $|V|$ -bit string  $\mathbf{z}_{jk}$  having a 1 only at positions  $j$  and  $k$ . Check whether  $d_{\mathbf{z}_{jk} \mathbf{z}_{jk}} = \pm e^{-i(\alpha_j + \alpha_k)}$  (the angles for the corresponding qubit in  $O$  is taken to be 0).
  - (i) if YES and the sign is  $-1$ , return  $E_{jk}$  as an edge in  $G$ .
  - (ii) if NO, no matching graph exists.

From Equation 3, we can see that a given phase map can be implemented by at most one pattern. Once an entanglement graph is obtained, we check whether  $(G, I, O)$  has a flow, in which case Theorem 1 obtains a deterministic pattern for  $U$ . We address the problem of finding a flow for the entanglement graph in the next section.

Although there are exponentially many elements on the diagonal of the phase map, testing for the existence of  $G$  will query the middle diagonal map only quadratically in  $|I| + n$ , to read off the measurement angles and the entanglement graph. This in practice could accelerate the detection of bad decompositions before obtaining all diagonal elements in the phase map.



When the procedure fails, because the obtained graph does not have flow or simply does not exist, one backtracks by: **(1)** trying a different decomposition given by Algorithm 1, **(2)** trying another solution from Lemma 2, **(3)** revising the choice of outputs, and ultimately **(4)** expanding further the computational space. Without any additional constraints, it seems that there are many solutions to be checked. One might be able to infer additional constraints to Equations 1 and 2 from the requirement that there be a corresponding entanglement graph, reducing the set of phase maps which we consider. How this may be done is, however, an open question.

## 6 Finding Flows

In this section, we outline algorithms which allow us to find flows for a geometry  $(G, I, O)$  in polynomial time. The proof of correctness of the algorithm employs technical results of graph theory, which we will only sketch here: a rigorous development may be found in [38].

### 6.1 Graph Theoretic Characterization of Flows

We will begin by showing how flows can be characterized in the language of graph theory, in order to make use of the solved problems in that field.

First, we present some additional notation related to directed paths. In a directed path, we write  $x \rightarrow y$  to represent an arc between vertices  $x$  and  $y$ . If  $\mathcal{C}$  is a collection of directed paths, we will say that  $x \rightarrow y$  is an *arc of  $\mathcal{C}$*  when  $x \rightarrow y$  is an arc in one of the elements of  $\mathcal{C}$ .

For a flow  $(f, \preceq)$ , we can easily see that the function  $f$  must be injective: if  $f(x) = f(y)$ , we have  $y \sim f(x)$  and  $x \sim f(y)$  by (Fi), and  $x \preceq y$  and  $y \preceq x$  by (Fiii), so  $x = y$ . Therefore, each vertex  $x \in V$  has at most one vertex  $w \in V$  such that  $x = f(w)$  and hence the orbits of vertices under the function  $f$  induce a path-like structure.

**Definition 3** *Let  $(G, I, O)$  be a geometry. A collection  $\mathcal{C}$  of (possibly trivial) directed paths in  $G$  is a path cover of  $(G, I, O)$  if*

- (i). *each vertex  $v \in V$  is contained in exactly one path;*
- (ii). *each path in  $\mathcal{C}$  is either disjoint from  $I$ , or intersects  $I$  only at its start point;*
- (iii). *each path in  $\mathcal{C}$  intersects  $O$  only at its end point.*

A path cover of  $(G, I, O)$  is meant to capture the way that information flows within the geometry during the execution of a pattern. When  $|I| = |O|$ , a path cover is just a maximum-size collection of directed paths from  $I$  to  $O$  which do not intersect (*i.e.* a *maximum family of vertex-disjoint  $I$ – $O$  paths*) which also happens to cover every vertex of the graph.

Every flow function  $f$  generates a path cover from its' orbits, and conversely we can obtain a natural function  $f$  from any path cover. However, not all path covers correspond to flows, because the function  $f$  from an *arbitrary* path cover may not have a compatible partial order satisfying (Fii) and (Fiii). For example, consider the geometry given by alternating input and output vertices on a cycle of length 6:

- $V = \{0, 1, 2, 3, 4, 5\}$ ,  $I = \{0, 2, 4\}$ , and  $O = \{1, 3, 5\}$ ;
- there is an edge between  $i, j \in V$  iff  $j - i \equiv \pm 1 \pmod{6}$ .

The only two path covers for  $(G, I, O)$  are generated by the functions  $f(x) \equiv x + 1 \pmod{6}$  and  $f(x) \equiv x - 1 \pmod{6}$ . In the former case, we have  $c_2 \sim f(c_0)$ ,  $c_4 \sim f(c_2)$ , and  $c_0 \sim f(c_4)$ : then, from condition (Fii), we would require  $c_0 \preceq c_2 \preceq c_4 \preceq c_0$ . Similarly, in the latter case, we would have  $c_0 \succ c_2 \succ c_4 \succ c_0$ . However, neither of these are possible if  $\preceq$  is a partial order.

In order to characterize when a path cover corresponds to a flow, we must introduce a condition which prohibits such a cycle of relations between distinct vertices. We do this by capturing the conditions which make a path cover give rise to these relations in the first place.

**Definition 4** Let  $\mathcal{F}$  be a family of directed paths in a graph  $G$ . A closed walk  $C = c_0 c_1 \cdots c_{m-1} c_0$  (indexed over  $\mathbb{Z}_m$ ) in  $G$  is a vicious circuit for  $\mathcal{F}$  if for all  $j \in \mathbb{Z}_m$ ,  $c_{j-1} \neq c_{j+1}$ , and at least one of  $c_{j-1} \rightarrow c_j$  or  $c_j \rightarrow c_{j+1}$  is an arc of  $\mathcal{F}$ .

That is: a vicious circuit is a walk that only visits vertices covered by  $\mathcal{F}$ , never doubles back on an edge which has just been traversed, and which traverses an arc of  $\mathcal{F}$  on at least one out of every two consecutive edges. The idea behind considering such a structure is that such a vicious circuit can be cut into segments, each consisting of one or two edges:

- **One edge segment:** an edge  $xy$ , where  $x \rightarrow y$  is an arc of  $\mathcal{F}$ ;
- **Two edge segment:** a path  $xyz$ , where  $x \rightarrow y$  is an arc of  $\mathcal{F}$ , but  $y \rightarrow z$  is not.

The importance of these segments is as follows. Let  $\mathcal{C}$  be a path cover, and  $f$  be the injective function naturally coming from it: then  $x \rightarrow y$  is an arc of  $\mathcal{C}$  iff  $y = f(x)$ . For any  $x$  and  $y$  which are the initial and final points of such a segment, any binary relation  $\preceq$  satisfying (Fii) and (Fiii) will have  $x \preceq y$ . As vicious circuits can be decomposed into such segments, a vicious circuit will then induce the cyclic relations we wish to prohibit. This motivates the following definition:

**Definition 5** A causal path cover of  $(G, I, O)$  is a path cover which does not have any vicious circuits in  $G$ .

The definition above is intended to simply exclude those path covers which induce cyclic relations of the sort above. In fact, this definition characterizes flows:

**Theorem 3 ([38], Corollary 11)** A geometry has a flow iff it has a causal path cover.

## 6.2 Uniqueness of Causal Path Covers among Families of Disjoint $I$ – $O$ paths

Theorem 3 tells us that in order to find a flow function  $f$  for a geometry  $(G, I, O)$ , we may replace the condition that  $f$  has a compatible partial order satisfying (Fii) and (Fiii) with the condition that the path cover induced by  $f$  lacks vicious circuits. In the special case where  $|I| = |O|$  (e.g. for a geometry from the pattern for a unitary transformation), we have the following result:

**Theorem 4 ([38], Theorem 16)** *Let  $(G, I, O)$  be a geometry such that  $|I| = |O|$ . If  $(G, I, O)$  has a causal path cover  $\mathcal{C}$ , then it is the only maximum family of vertex-disjoint  $I$ – $O$  paths in  $G$ .*

The reason for this is that any other maximum family of vertex-disjoint  $I$ – $O$  paths either fails to cover all vertices of  $G$ , or traverses a different set of edges in  $G$ . From this, one can prove that a vicious circuit must exist for  $\mathcal{C}$ . Thus, if  $\mathcal{C}$  is causal, no other maximum family of vertex-disjoint  $I$ – $O$  paths may exist. As a corollary, because a causal path cover for  $(G, I, O)$  is unique when it exists, a geometry  $(G, I, O)$  has at most one possible flow function.

Using the above result, if  $(G, I, O)$  has a flow, we may find it by first finding any maximum family of vertex-disjoint  $I$ – $O$  paths, which has a known reduction to the Maximum Integral Flow problem.

### 6.3 Reduction to Maximum Integral Flow

Informally, an integral flow network consists of a directed graph  $N$ , together with a single *source vertex*  $r$  and a single *sink vertex*  $s$ , and where each arc  $x \rightarrow y$  in  $N$  has an associated capacity  $c(x \rightarrow y) \in \mathbb{N}$ . We are interested in sending some measurable commodity from the source to the sink, under the constraints that

- (i). the commodity can only be sent between vertices in the direction of an arc;
- (ii). any amount of the commodity which enters a vertex other than the sink must also leave that vertex;
- (iii). the amount of commodity sent over an arc is at most the capacity of the arc.

In particular, we are interested in possible *network-flow functions*  $u$ , where  $u(a) \in \mathbb{N}$  gives the amount of the commodity which we send across the arc  $a$ . Define

$$F_u(x) = \left[ \sum_{(w \rightarrow x)} u(w \rightarrow x) \right] - \left[ \sum_{(x \rightarrow y)} u(x \rightarrow y) \right] : \quad (4)$$

then, the conditions above state that  $F_u(x) = 0$  for  $x \notin \{r, s\}$ , and that for each arc  $a$ , we have  $u(a) \leq c(a)$ . The Maximum Integral Flow problem is to find a network-flow  $u$  such that  $F_u(s)$  is maximal: this has several known efficient solutions which are commonly implemented in programming libraries. We will not discuss them here except for the purpose of run-time analysis: interested readers may refer to [39] or [40].

To reduce finding a maximum family of vertex-disjoint  $I$ – $O$  paths to Maximum Integral Flow, we use the following standard network construction:

**Definition 6** *Let a geometry  $(G, I, O)$  be fixed. Define a digraph  $N$  with the vertices*

- $\mathcal{A} = \{A_v \mid v \in I \cup O^c\}$  (out-flow vertices);
- $\mathcal{B} = \{B_v \mid v \in O \cup I^c\}$  (in-flow vertices), *such that  $A_v = B_v$  iff  $v \in I \cap O$ ;*
- *a source vertex  $r$  and a sink vertex  $s$ ,*

*and with the following arcs:*

- For  $i \in I$ ,  $A_i$  has only the incoming arc  $r \rightarrow A_i$ ; all other in-take vertices  $A_v$  have only the incoming arc  $B_v \rightarrow A_v$ .
- For  $\omega \in O$ ,  $B_\omega$  has only the outgoing arc  $B_\omega \rightarrow s$ ; all other out-take vertices  $B_v$  have only the outgoing arc  $B_v \rightarrow A_v$ .
- If  $v \in O^c$  and  $w \in I^c$ , there is an arc  $A_v \rightarrow B_w$  iff  $vw \in G$ .

We call  $N$  the max-flow digraph of  $(G, I, O)$ .

The purpose of defining this network is to force any network flow function  $u$  on the arcs of  $N$  to describe a collection of paths from  $r$  to  $s$  in  $D$ , from which we can obtain a family of vertex-disjoint  $I$ – $O$  paths in  $G$ . We will now describe how this construction can be used to find such a maximum family of paths.

For the case where  $I$  and  $O$  are disjoint, consider the network that would be obtained by adding source and sink vertices  $r$  and  $s$  to  $V$ , replacing each edge  $xy \in E$  with arcs  $x \rightarrow y$  and  $y \rightarrow x$ , adding arcs  $r \rightarrow i$  and  $\omega \rightarrow s$  for all  $i \in I$  and  $\omega \in O$ . If we set the capacities of all arcs in  $N$  equal to 1, then a maximum integral flow in  $N$  could be represented by a set  $S$  of arcs  $a$  in  $N$  for which  $u(a) = 1$ . From the condition  $F_u(x) = 0$  for  $x \notin \{r, s\}$ , each vertex other than  $r$  or  $s$  would have the same number of arcs in  $S$  which enter it as it does that leaves it. Then, the arcs in  $S$  describe a collection of *edge-disjoint* paths from  $r$  to  $s$ , and this collection of paths is at a maximum when  $u$  is a maximum integral flow.

To force *vertex-disjointness*, we want at most one arc of  $S$  to enter each vertex, and at most one arc of  $S$  to leave each vertex. We can do this by replacing each vertex  $x$  by two vertices  $B_x \rightarrow A_x$ , where all arcs which left  $x$  now leave  $A_x$ , and all arcs which entered  $x$  now enter  $B_x$ . Because only one arc leaves  $B_x$ , at most one arc of  $S$  can enter  $B_x$ ; and similarly with arcs leaving  $A_x$ . Having a maximum family of vertex-disjoint paths in  $N$  from  $r$  to  $s$ , we can recover a maximum family of vertex-disjoint paths in  $G$  by removing  $r$  and  $s$ , and contracting all pairs  $\{B_x, A_x\}$  to a single vertex  $x \in V$ .

For the case where  $I$  and  $O$  are not disjoint, we can let  $A_x$  and  $B_x$  be equal when  $x \in I \cap O$ , as long as we do not connect  $x$  to any vertices other than  $r$  or  $s$ . The network that results will be the max-flow digraph  $N$  described in Definition 6 above.

Given a geometry  $(G, I, O)$  the max-flow digraph for  $(G, I, O)$  can easily be constructed in  $O(m)$  time. Then, by the above construction, we can attempt to find a path cover for  $(G, I, O)$  as follows:

**Algorithm 3** Input: the max-flow digraph  $N$  of a geometry  $(G, I, O)$ , with arc capacities set to 1 for each arc of  $N$ .

Output: either (i) a path cover  $\mathcal{C}$  for  $(G, I, O)$  and a function  $f : O^c \rightarrow I^c$  whose orbits induce the paths in  $\mathcal{C}$ , or (ii) no flow exists for  $(G, I, O)$ .

1. Set  $u$  to be a maximum integral network flow for  $N$ .
2. Find a family  $\mathcal{C}$  of directed paths in  $G$  which start at input vertices, end at output vertices, and only traverses edges  $xy$  such that  $u$  is non-zero on the arc  $A_x \rightarrow B_y$ .
3. For each arc  $A_x \rightarrow B_y$  of  $\mathcal{C}$ , set  $f(x) = y$ .
  - (i) If the paths of  $\mathcal{C}$  cover all vertices of  $G$ , return  $(\mathcal{C}, f)$ .
  - (ii) Otherwise, no flow exists for  $(G, I, O)$ .

Whether or not  $(G, I, O)$  has a flow, the collection of paths  $\mathcal{C}$  which is constructed will be a maximum family of vertex-disjoint  $I$ – $O$  paths; we can check if they cover  $V$  (and construct the function  $f$ ) by simply traversing the paths. By Theorem 4, if  $\mathcal{C}$  doesn't cover all vertices, then  $(G, I, O)$  has no causal path cover, in which case it also has no flow.

Let  $n = |V|$ ,  $m = |E|$ , and  $k = |I| = |O|$ . The Maximum Integral Flow problem on  $N$  can be solved in time  $O(km)$  by the Ford-Fulkerson algorithm (see, e.g. [39]). The time required to construct  $\mathcal{C}$  and  $f$ , and to verify that  $\mathcal{C}$  is a path cover, will be  $O(n)$ . Thus the running time of Algorithm 3 is  $O(km)$  when  $G$  is a connected graph.

#### 6.4 Obtaining the Dependency Order of $f$

The function  $f$  returned as part of Algorithm 3 is necessary, but not sufficient, for  $(G, I, O)$  to have a flow. We must also discover if  $f$  has a compatible partial order which satisfies (Fii) and (Fiii). Suppose that  $f$  has such a compatible partial order, and consider in particular the dependency order  $\preceq$  of  $f$ . Because it is the coarsest compatible order,  $\preceq$  can be defined as the transitive closure of the binary relation  $\partial$  on  $V$ , given by

$$x \partial y \implies [y = x] \vee [y = f(x)] \vee [y \sim f(x)], \quad (5)$$

which we will call the *dependency relation*: we will say that  $y$  *depends* on  $x$  if  $x \partial y$ . We can then reduce finding the dependency order to the Transitive Closure problem, which is concerned precisely with finding the transitive closure of binary relations.<sup>2</sup> If there is a cycle of dependency relations, then the transitive closure of  $\partial$  will not be a partial order, in which case  $f$  is not a flow function; otherwise,  $f$  is a flow function, and the transitive closure will be the dependency relation of  $f$ .

Algorithm 4 is a Tarjan-like algorithm for detecting cycles in the dependency relation  $\partial$  (given the function  $f$  and graph  $G$  which determines  $\partial$ ), and computing the transitive closure if no such cycles exist. It also takes the path cover  $\mathcal{C}$  as input.

**Algorithm 4** Input: A geometry  $(G, I, O)$ , and the output  $(\mathcal{C}, f)$  of Algorithm 3.  
Output: either (i) the dependency order  $\preceq$  of  $f$ , or (ii) no flow exists for  $(G, I, O)$ .

- Let **sup** be an array mapping pairs  $(x, P) \in V \times \mathcal{C}$  to the supremum (i.e. the least upper bound) of the set  $\{x\}$  in the path  $P$ , or the empty set if there is no least upper bound.<sup>3</sup> Initialize **sup** $[x, P] = \emptyset$  for all  $(x, P) \in V \times \mathcal{C}$ .
- Let **status** be an array mapping  $x \in V$  to one of **{none, pending, fixed}**; where **status** $[x] = \text{none}$  indicates that no supremum of  $\{x\}$  has yet been discovered, and **status** $[x] = \text{fixed}$  indicates that all suprema of  $\{x\}$  have been discovered. Initialize **status** $[x] = \text{none}$  for all  $x \in V$ .

<sup>2</sup> The Transitive Closure problem is usually expressed in terms of directed graphs, but doing so doesn't provide any additional insight into the problem, and is at any rate equivalent to the problem for binary relations.

<sup>3</sup> In the literature for the Transitive Closure problem, this is known as a *chain decomposition* of the directed graph represented by the relation  $\partial$ .

- For each vertex  $x \in V$  with  $\mathbf{status}[x] = \mathbf{none}$  perform the following recursive algorithm to set the suprema of  $\{x\}$ :
  1. Set  $\mathbf{status}[x] = \mathbf{pending}$ .
  2. For the path  $P_x$  which contains  $x$ , set  $\mathbf{sup}[x, P_x] = x$ .
  3. For each vertex  $y$  which depends on  $x$  (aside from  $x$  itself):
    - if  $\mathbf{status}[y] = \mathbf{none}$ , recursively determine the suprema of  $\{y\}$ .
    - if after this  $\mathbf{status}[y] \neq \mathbf{fixed}$ ,  $(G, I, O)$  has no flow; abort.
    - otherwise, set  $\mathbf{sup}[x, P] = \min(\mathbf{sup}[x, P], \mathbf{sup}[y, P])$  for each path  $P \in \mathcal{C}$  (taking the minimum with respect to distance from the start of  $P$ ).
  4. Set  $\mathbf{status}[x] = \mathbf{fixed}$ .
- Once  $\mathbf{status}[x] = \mathbf{fixed}$  for all  $x \in V$ , return the array  $\mathbf{sup}$ .

This algorithm determines if there is a cycle of dependencies by performing a depth-first search, and checking if it traverses a sequence of relations  $x \partial y \partial \dots \partial x$  in the course of finding the elements which are greater than  $x$  in the dependency order. If it does, it will discover that  $\mathbf{status}[x] = \mathbf{pending}$  on the second time it visits  $x$ : then, it may as well abort, as  $f$  cannot be a flow function and no dependency order exists.

The array  $\mathbf{sup}$  returned as output characterizes the dependency order  $\preceq$ : we have  $x \preceq y$  if and only if  $\mathbf{sup}[x, P_y] \leq y$ , where  $P_y$  is the path containing the vertex  $y$ , and the inequality  $\leq$  is with respect to the distance from the initial vertex of  $P_y$ . We can compute this easily by constructing functions which maps each vertex  $y \in V$  to an index for  $P_y$ , and another function mapping each vertex  $x \in V$  to the distance of  $x$  from the initial point of  $P_x$ . This can be considered as a part of building the path cover  $\mathcal{C}$  in Algorithm 3 (indeed, such functions characterize the path cover  $\mathcal{C}$  and may be considered to be how  $\mathcal{C}$  is represented).

Let  $n = |V|$ ,  $m = |E|$ , and  $k = |I| = |O| = |\mathcal{C}|$ . The time required to fix the values of  $\mathbf{sup}[x, P]$  for each path  $P \in \mathcal{C}$  is  $O(k \deg(x))$ . Summing over all  $x \in V$ , the cost of recursively obtaining the suprema for all of  $V$  is  $O(km)$ . This is then the cost of Algorithm 4 as a whole, as initializing  $\mathbf{sup}$  and  $\mathbf{status}$  takes a total of  $O(kn) \subseteq O(km)$  time for  $G$  connected.

## 7 Discussion and Conclusion

We have presented a decomposition of unitary maps into three successive operations  $P$ ,  $\Phi$ , and  $R$ . The first one represents the familiar preparation map and expands the computation space by introducing auxiliary qubits; the second one is diagonal in the computational basis and has only unit coefficients; and the last is a restriction map that contracts back the computational space into the chosen output space. It is important to emphasize that both  $R$  and  $P$  have a very simple structure, and hence the decomposition suggests that the whole quantum computing part of an algorithm is encoded in the phase map operator.

The restriction map  $R$  does not correspond directly to a meaningful physical transformation, so this decomposition is a mathematical artifact. However, we have illustrated how one may attempt to find a one-way patterns which effectively implements such phase decompositions. We have also shown how one may attempt to find a phase

map decomposition directly. This constitutes a method for the implementation of unitary maps in the one-way model which completely bypasses the circuit model. It is hoped that the phase map decomposition may produce more efficient implementations in particular instances.

An interesting restriction which may be imposed is to restrict the choice of the allowed angles. For example, we might restrict to multiples of  $\pi/4$ , in the hope of staying within the world of Pauli measurements and the so-called  $\pi/4$  magic preparations, which may help with implementations [17]. In this restricted case, the Equations of Lemma 2 may no longer have an exact solution in general; however, one does not expect an exact solution in this case, since the obtained model is only approximately universal. It would be interesting to see whether one can compute down an approximate phase map decomposition such that  $U \approx R \circ \Phi \circ P$  with arbitrary precision.

Another question is whether there is a reasonable relaxation of the definition of a pattern, by allowing new commands which would allow additional possible phase maps. How much a non-trivial extension would complicate the theory (*e.g.*, standardization, flow) and the implementation (*e.g.*, requiring only one simple primitive for entanglement) of one-way patterns is not clear.

## References

1. D. Gottesman and I. L. Chuang. Quantum teleportation is a universal computational primitive. *Nature*, 402:390, 1999.
2. R. Raussendorf and H.-J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86(5188), 2001.
3. R. Raussendorf, D. E. Browne, and H.-J. Briegel. Measurement-based quantum computation on cluster states. *Phys. Rev. A*, 68(022312), 2003.
4. M. A. Nielsen. Universal quantum computation using only projective measurement, quantum memory, and preparation of the 0 state. *Phys. Lett. A.*, 308:96, 2003.
5. D. Schlingemann. Cluster states, algorithms and graphs. quant-ph/0305170, 2003.
6. M. Hein, J. Eisert, and H.-J. Briegel. Multi-party entanglement in graph states. *Phys. Rev. A*, 69:62311, 2004.
7. W. Dür, H. Aschauer, and H.-J. Briegel. Multiparticle entanglement purification for graph state. *Phys. Rev. Lett.*, 91:107903, 2003.
8. M. Van den Nest, J. Dehaene, and B. De Moor. Graphical description of the action of local clifford transformations on graph states. *Phys. Rev. A.*, 69:0223116, 2004.
9. M. Van den Nest, J. Dehaene, and B. De Moor. An efficient algorithm to recognize local clifford equivalence of graph states. *Phys. Lett. A.*, 70:034302, 2004.
10. M. Mhalla and S. Perdrix. Complexity of graph state preparation. quant-ph/0412071, 2004.
11. D. W. Leung. Quantum computation by measurements. *IJQI*, 2(1), 2004.
12. P. Aliferis and D. W. Leung. Computation by measurements: a unifying picture. *Phys. Rev. A*, 70:062314, 2004. quant-ph/0404082.
13. A. M. Childs, D. W. Leung, and M. A. Nielsen. Unified derivations of measurement-based schemes for quantum computation. quant-ph/0404132, 2004.
14. S. Perdrix and P. Jorrand. Measurement-based quantum turing machines and their universality. quant-ph/0404146, 2004.
15. P. Jorrand and S. Perdrix. Unifying quantum computation with projective measurements only and one-way quantum computation. quant-ph/0404125, 2004.

16. V. Danos, E. Kashefi, and P. Panangaden. The measurement calculus. quant-ph/0412135, 2004.
17. V. Danos and E. Kashefi. Pauli measurements are universal. In Peter Selinger, editor, *Proceedings of the 3rd International Workshop on Quantum Programming Languages, QPL 2005, Chicago*. ENTCS, June 2005.
18. T. Rudolph and S. S. Virmani. A relational quantum computer using only two-qubit total spin measurement and an initial supply of highly mixed single qubit states. quant-ph/0503151, 2005.
19. R. Raussendorf, Simon Anders, and H.-J. Briegel. Fault-tolerant quantum computation using graph states. Communication to the Quantum Information and Quantum Control Conference, Fields Institute, Toronto. <http://atlas-conferences.com/c/a/n/n/80.htm>, July 2004.
20. M. A. Nielsen and C. M. Dawson. Fault-tolerant quantum computation with cluster states. quant-ph/0405134, 2004.
21. R. Raussendorf, S. Bravyi, and J. Harrington. Long-range quantum entanglement in noisy cluster states. *Phys. Rev. A*, 71:062313, 2004.
22. P. Aliferis and D. W. Leung. Fault-tolerant quantum computation in the graph-state model. quant-ph/0503130, 2005.
23. M. Varnava, D. E. Browne, and T. Rudolph. Loss tolerant one-way quantum computation – a horticultural approach. quant-ph/0507036, 2005.
24. R. Raussendorf, J. Harrington, and K. Goyal. fault-tolerant one-way quantum computer. quant-ph/0510135, 2005.
25. C. M. Dawson, H. L. Haselgrove, and M. A. Nielsen. Noise thresholds for optical quantum computers. quant-ph/0509060, 2005.
26. M. A. Nielsen. Optical quantum computation using cluster states. *Phys. Rev. Lett.*, 93(4):040503, 2004.
27. S.R. Clark, C. Moura Alves, and D. Jaksch. Efficient generation of graph states for quantum computation. *New J. Phys.*, 7(124), 2005.
28. D. E. Browne and T. Rudolph. Resource-efficient linear optical quantum computation. *Phys. Rev. Lett.*, 95:010501, 2005.
29. M. S. Tame, M. Paternostro, M. S. Kim, and V. Vedral. Toward a more economical cluster state quantum computation. quant-ph/0412156, 2004.
30. M. S. Tame, M. Paternostro, M. S. Kim, and V. Vedral. Natural three-qubit interactions in one-way quantum computing. quant-ph/0507173, 2005.
31. P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger. Experimental one-way quantum computing. *Nature*, 434:169–176, March 2005.
32. A. Kay, J. K. Pachos, and C. S. Adams. Graph state preparation and cluster computation with global addressing of optical lattices. quant-ph/0501166, 2005.
33. S.C. Benjamin, J. Eisert, and T.M. Stace. Optical generation of matter qubit graph states. *New J. Phys.*, 7:194, 2005.
34. Q. Chen, J. Cheng, K. Wang, and J. Du. Efficient construction of 2-d cluster states with probabilistic quantum gates. quant-ph/0507066, 2005.
35. S. C. Benjamin, D. E. Browne, J. Fitzsimons, and J. J. L. Morton. Brokered graph state quantum computing. quant-ph/0509209, 2005.
36. V. Danos and E. Kashefi. Determinism in the one-way model. quantph-0506062, 2005.
37. V. Danos, E. Kashefi, and P. Panangaden. Robust and parsimonious realisations of unitaries in the one-way model. *Phys. Rev. A*, 72, 2005.
38. N. de Beaudrap. Characterizing & constructing flows in the one-way measurement model in terms of disjoint  $I-O$  paths. quant-ph/0603072, 2006.
39. T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction to Algorithms*. MIT Press and McGraw-Hill, 2001. 2nd edition.



40. W. J. Cook, W. H. Cunningham, W. R. Pulleybank, and A. Schrijver. *Combinatorial Optimization*. Wiley-Interscience New York, 1998. Section 3.2, pages 38–45.